Nr. 61

GEHEIM - SECRET

Der Chef
des Uebermittlungsdienstes der Armee

Le Chef
du Service des Transmissions de l'Armée

SCHLUESSELUNGSVERFAHREN
für die
NEMA-MASCHINE.

PROCEDE DE CHIFFREMENT
pour la
MACHINE NEMA.

Ausgabe Mai 1948

Edition mai 1948

1. DER GEHEIME SCHLUESSEL wird durch Schlüsselbefehl ausgegeben. Die Dauer seiner Gültigkeit richtet sich nach dem Verkehr und wird von Fall zu Fall befohlen.

   Er besteht aus zwei Teilen:

   a) dem innern Schlüssel, der die Reihenfolge der Kontakt- und Fortschaltewalzen bestimmt , welche wie folgt angegeben wird:

      11A - 15F - 120 - 148

      Die Buchstaben bedeuten die Kontaktwalzen, auf welche die Fortschaltewalzen (durch zweistellige Zahlen gekennzeichnet) links aufgeschoben werden.

   b) einem Schlüsselwort, mit dessen Hilfe gemäss untenstehender Vorschrift der äussere Schlüssel gewonnen wird. Das Schlüsselwort soll 10 oder mehr Buchstaben enthalten, z. B.:

      Z A R U N D Z I M M E R M A N N

2. VORSCHRIFT ZUR GEWINNUNG DES AEUSSERN SCHLUESSELS.

   Zur Gewährleistung der kryptographischen Sicherheit muss jedes Telegramm mit einem andern äussern Schlüssel chiffriert werden.

   a) An der Maschine mit dem zur Zeit geltenden innern Schlüssel werden die 10 ersten Buchstaben des geheimen Schlüsselwortes an den Buchstabenkränzen von links nach rechts eingestellt.

   b) Der Chiffreur schreibt 10 von ihm beliebig gewählte Buchstaben in Form von 2 Fünfergruppen als Anfang des Chiffrates auf. Diese Buchstabenfolge wird am Schluss des Chiffrates wiederholt.

c) Mit der nach a) bereitgestellten Maschine werden die 10 Buchstaben chiffriert und auf einen besondern Zettel notiert.

d) Die so gewonnene Buchstabengruppe wird als äusserer Schlüssel an der Maschine eingestellt, der Zähler auf Null gebracht,und die Maschine ist bereit zur Chiffrierung oder Dechiffrierung der Meldung.

Für den Dechiffreur fällt die Wahl der 10 Buchstaben nach b) dahin. Er entnimmt dem ankommenden Telegramm di 10 ersten Buchstaben, kontrolliert und vergleicht sie mit den letzten 10 Buchstaben des Chiffrates und verfährt im übrigen nach obiger Vorschrift. Bei Nichtübereinstimmung werden zunächst die am Anfang stehenden Bechstaben zur Gewinnung des äussern Schlüssels benützt. Ergibt dies beim Dechiffrieren der Meldung keinen Klartext, so sind die am Ende stehenden Buchstaben zu verwenden. Führt auch dies nicht zum Ziel, so ist die Wiederholung der ersten beiden Gruppen vom Absender zu verlangen.

3. CHIFFRIEREN UND DECHIFFRIEREN. (Die technische Seite wird in der Bedienungsanleitung zur Chiffriermaschine " N e m a " behandelt.)

a) Der Chiffretext der Meldung schliesst an die unter 2b) erwähnten zwei Schlüsselgruppen an und wird in Fünfergruppen geordnet. Bei unvollständiger letzter Fünfergruppe wird nicht aufgeblendet. Die 10 Buchstaben der beiden Schlüsselgruppen werden anschliessend wiederholt, womit das Chiffrat beendigt ist. Beim Dechiffrieren werden die ersten beiden Gruppen und die letzten 10 Buchstaben als zum Schlüssel gehörig weggelassen.

b) Die Anzahl der Buchstaben des Chiffretextes ohne Schlüsselgruppen muss stets mit der Zählerangabe übereinstimmen.

c) Wird beim Chiffrieren ein Fehler begangen, der sinnstörend wirkt, und kann er nicht nach dem in der Bedienungsanleitung beschriebenen Verfahren korrigiert werden, so wird die den Fehler enthaltende Partie noch einmal anschliessend richtig chiffriert, wobei im Chiffrat der den Fehler aufweisende Teil stehen bleiben muss. Beim Dechiffrieren gilt die Wiederholung als richtig.

d) Zahlen werden mit Y angezeigt und getrennt. Der Uebergang zu Buchstaben wird mit X bezeichnet, wie auch die Trennung von Worten, wenn eine solche sich als absolut notwendig erweist.

4. BEISPIEL.

a) Geheimer Schlüssel: 11A - 15F - 12D - 14B
ZAR UND ZIMMERMANN

b) An der Maschine wird eingestellt: ZARUNDZIMM

c) Wahl der zu übermittelnden Schlüsselgruppen: Q Z A F J T M C A R

d) Chiffrat dieser Gruppen: Z Q L M K A L R Q U wird an der Maschine eingestellt, Zähler auf Null gebracht, und die Maschine ist zum Chiffrieren oder Dechiffrieren der Meldung bereit.

e) Chiffretelegramm:

Adresse: . . . . . Chi: . . . . . .
Q Z A F J T M C A R . . . . . .
. . . . . Q Z A F J T M C A R

Unterschrift: . . . . . .

1. LA CLEF SECRETE est émise par ordre de clef. Sa durée dépendra du trafic et sera commandée pour chaque cas individuellement.

La clef secrète se compose de deux parties:

a) de la clef intérieure, laquelle détermine l'ordre des disques de contact et des couronnes de propulsion. Cet ordre est indiqué de la façon suivante:

11A - 15F - 12D - 14B

Les lettres désignent les disques de contact; à leur gauche se logent les couronnes de propulsion (indiquées par des nombres composés de deux chiffres);

b) d'un mot-clef au moyen duquel on forme la clef extérieure (voir l'instruction ci-dessous). Par ex.:

R O M A I N R O L L A N D

2. INSTRUCTION POUR L'OBTENTION DE LA CLEF EXTERIEURE.

Pour le rendre sûr au point de vue cryptographique, la clef extérieure doit être changée à chaque télégramme.

a) La machine se trouvant au point, c'est-à-dire les disques étant réglés selon la clef intérieure valable au moment du chiffrement ou du déchiffrement, on forme la clef extérieure en alignant de gauche à droite sur les couronnes de lettres des 10 premières lettres du mot-clef secret.

b) Le chiffreur note, comme début du cryptogramme, 10 lettres quelconques qui doivent être écrites en deux groupes de 5 lettres. On répétera ces 10 lettres, dans le même ordre, à la fin du message.

c) Ces lettres sont chiffrées sur la machine préparée selon lettre a) ci-dessus et l'on note le résultat sur une feuille détachée.

d) Le groupe de lettres ainsi obtenu doit être placé sur la machine comme clef extérieure; le compte-

lettres est amené à zéro; la machine est prête au chiffrement et au déchiffrement.

Le déchiffreur n'aura pas à choisir les 10 lettres dont il est question sous lettre b). Il comparera tout simplement les 10 premières lettres du cryptogramme aux 10 dernières et agira en outre comme il est indiqué ci-dessus. Si les 10 lettres du début ne concordent pas avec celles de la fin, le déchiffreur se servira tout d'abord des lettres du début en vue d'obtenir la clef extérieure. Si, par ce procédé, il n'obtient pas de texte clair en déchiffrant le message, il utilisera les 10 dernières lettres. Si, malgré cela, il n'y a pas de résultat, le déchiffreur demandera à l'expéditeur la répétition des 2 premiers groupes.

3. CHIFFREMENT ET DECHIFFREMENT. (Le côté technique est traité dans l'"Instruction de service de la machine N e m a".)

a) Le texte chiffré du message suit les deux groupes de clef de 5 lettres mentionnées sous 2b); on y ajoute immédiatement après les 10 lettres figurant dans les deux groupes de clef de 5 lettres du début et on divise le tout en groupes de 5 lettres; seul le dernier groupe peut compter moins de 5 lettres; il ne sera pas complété. En déchiffrant, il ne faudra pas tenir compte des 10 premières et des 10 dernières lettres du message, puisqu'elles font partie de la clef.

b) Le nombre de lettres du cryptogramme (sans les groupes de clef) doit correspondre au chiffre que le compte-lettres indique.

c) Si, en chiffrant on s'est trompé d'une façon qui pourrait troubler le sens du message et si cette erreur ne peut pas être corrigée de la manière indiquée dans l'"Instruction de service", la partie contenant la faute sera chiffrée une deuxième fois; la partie contenant l'erreur doit être laissée dans le cryptogramme. C'est la partie répétée qui comptera pour le déchiffreur.

d) Les chiffres doivent être précédés et séparés par un Y. Le passage aux lettres par contre sera indiqué par X, de même la séparation de mots, là où elle est absolument nécessaire.

4. EXEMPLE.

a) Clef secrète: 11A - 15F - 12D - 14B
ROMAIN ROLLAND

b) La machine sera mise sur: ROMAINROLL

c) Groupes de clef choisis pour la transmission: Q Z A F J T M C A R

d) Le cryptogramme de ces groupes: E M Z E K A C T L X est placé sur la machine, le compte-lettres est ramené à zéro et la machine est prête au chiffrage ou déchiffrage du message.

e) Télégramme chiffré:
Adresse: . . . . . Chi: . . . . . .
Q Z A F J T M C A R . . . . . .
. . . . . Q Z A F J T M C A R

Signature: . . . . . .